Administrative Policies and Procedures: 9.4

Subject:	**Confidential Child-Specific Information**
Authority:	TCA 36-1-125, 36-1-126; 37-1-153; 37-1-409; 37-1-612; 37-2-408; 37-5-105; 37-5-106; 37-5-107
Standards:	**ACA:** 3-JTS-1C-24, 3-JTS-1E-07; **COA:** PA-CR2, PA-RPM 2, PA-RPM 6, PA-TS 2.02; **DCS Practice Model Standard**: 7-102A, 8-306
Application:	To All Department of Children's Services Employees and Contract Service Providers

Policy Statement:

DCS shall ensure that all information created or data collected, directly or indirectly, in any medium, which identifies a child and their family, shall be kept confidential in order to protect their privacy. Child case files and related information are official records which have been designated confidential by law and will be safeguarded in accordance with applicable statutes, rules, policies, and ethical standards.

Purpose:

To establish procedures to ensure that child-specific information is kept confidential in order to protect the privacy of clients and their families.

Procedures:

A. Safeguarding of confidential information

1. **Paper**

   a) Client records and files will be stored in locked rooms or storage systems as outlined in DCS policies ***9.2, Youth Case Files in DCS Community Residential Facilities; 9.3 DOE, Standardization and Confidentiality of Student Master Files; 31.5, Regional Child Case Files*** and applicable ***DCS Health Insurance Portability and Accountability Act of 1996 (HIPAA) policies***. Where lockable storage is not available, other reasonable measures must be taken to safeguard confidential information.

   b) All pending, open, or closed child case file record information will be maintained in secure conditions that guarantee confidentiality, integrity, and availability to authorized individuals and agencies when needed.

   c) Confidential record information will be labeled ***"CONFIDENTIAL"*** and maintained in secure shelf/cabinet/storage areas or possess computerized "built-in" security features to prevent access by unauthorized users. Reasonable precautions, including safeguards from tampering, theft, fire or water damage, environmental hazards, and natural disasters, will be initiated.

	2. **Verbal** a) DCS staff must take reasonable measures to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs. b) Enclosed offices, interview rooms or other secure locations will be available for the verbal exchange of confidential information. **3. Visual/electronic** a) DCS staff must ensure that observable confidential information on computer screens is adequately shielded from unauthorized disclosure. Suggested means for ensuring this protection include: ♦ Use of polarized screens or other computer screen overlay devices that shield information on the screen; ♦ Placement of computers out of the visual range of persons other than the authorized user; ♦ Clearing information from the screen when not actually being used; Locking-down computer work stations when not in use; and ♦ Other effective means as available. b) DCS staff must safeguard and provide minimum necessary access to paper documents containing confidential information that are located on: ♦ Desks ♦ Fax machines; ♦ Photocopy machines; ♦ Portable electronic devices (e.g., laptop computers, palm pilots, etc.); ♦ Computer printers; ♦ Removable media (e.g., diskettes, CDs, etc.); and ♦ Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).
B. Release of information	The release of confidential information of a child and his/her family shall be in accordance with DCS policy ***9.5, Access and Release of Confidential Child-Specific Information.***
C. Record security and recovery	1. Information backups are essential in the event of an emergency or disaster. Therefore, DCS management will ensure that cost effective record security, disaster preparedness and recovery procedures are prepared, implemented, and reviewed annually. 2. The security and recovery of open, inactive, and closed automated child record data will be at the direction of the DCS Office of Information Systems (OIS) based on information owner/user feedback and applicable Records Disposition Authorization (RDA). 3. Formalized security controls and procedures for sensitive and privileged child data provided in electronic communication systems, such as e-mail and the

	Internet, will be coordinated by DCS-OIS. 4. DCS shall also comply with federal regulations, court mandates, legal settlements, and accreditation standards concerning the confidentiality of child-specific record information.
D. Records disposition	1. Confidential health/medical, educational, foster care, adoption, and CPS record information will be dispositioned in accordance with the applicable RDA. 2. All other contents such as social histories, face sheets, permanency plans, psychological reports by other agencies, incident reports, court orders, police records, photographs, and any other confidential record not specified for retention will be removed and held in a secured location pending proper destruction. 3. Confidential electronic files will be dispositioned in accordance with the applicable RDA. 4. Child health/medical and educational records are vital components of the case record and may be maintained separately, regardless of media, in other appropriate and secure areas within DCS facilities, in accordance with applicable RDA and DCS policies. 5. DCS will secure an appropriate media format for any confidential record mandated by statute for preservation, such as sealed adoption files. 6. Retaining records after the expiration of their retention period for the sole purpose of convenience will jeopardize the credibility of the department records retention program. Therefore, DCS will not retain confidential information that duplicates other "official" records, such as birth/death certificates, social security cards, etc., maintained permanently by other governmental entities.
E. Records destruction	1. Secure storage, timely retention, and proper disposal of confidential record information will be handled in accordance with applicable RDA and DCS policies. 2. Files and documents awaiting disposal or destruction in desk-site containers, lockable storage rooms, or centralized waste/shred bins, will be appropriately labeled and destroyed on a regular basis consistent with record retention requirements. 3. DCS workplaces that do not have lockable storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to confidential information. 4. Approved methods for destroying confidential paper record information are shredding, burning and acid bath recycling. Erasure of electronic record information will be at the direction of the DCS-OIS in accordance with applicable DCS policy. 5. Form ***GS-0989, Department of General Services Certificate of Records Destruction***, must be completed and forwarded to the appropriate records clerk/coordinator and to the departmental records officer.

Forms:	***GS-0989, Department of General Services Certificate of Records Destruction***

Collateral documents:	*None*